Privacy Guidelines Committee Guidance Paper
Suggested Approach for Applying the
Information Sharing Environment Privacy Guidelines

This paper is designed to provide the Privacy Guidelines Committee (PGC) with a workable approach for applying the Information Sharing Environment (ISE) Privacy Guidelines to systems of records and databases ("systems" is used herein to refer to information systems, databases, and data sets, as appropriate) that contain information within the scope of the ISE.

Background:

This approach relies on the definitions of "terrorism information (TI)," "homeland security (HS) information," and "law enforcement (LE/T) information" (hereafter collectively referred to as terrorism information) contained in Guideline 2—Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector (attached for reference) and Guideline 5—Guidelines to Implement Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines). The approach further recognizes the "process" nature of the ISE Privacy Guidelines and their specific process requirements. The approach, described below, also recognizes the ISE goal of facilitating, coordinating, and expediting access to protected terrorism information.

Although the definitions in Guideline 2 and Guideline 5 clearly delineate the types of information covered within the ISE and the ISE Privacy Guidelines, more guidance is needed on how ISE privacy officials are to apply these definitions to their agencies' systems and sharing arrangements.

In general, privacy law is centered upon an analysis of collections of personally identifiable information. In particular, the Privacy Act, which applies to all federal agencies, including Intelligence Community elements, contains a set of requirements for "systems of records." The PGC has been seeking to clarify and understand the process that agencies are expected to follow in determining the systems and sharing arrangements that are either currently considered to be part of the ISE or are contemplated to become part of the ISE. Once that process is defined, ISE privacy officials can focus on applying the requirements of the ISE Privacy Guidelines to those systems and arrangements.

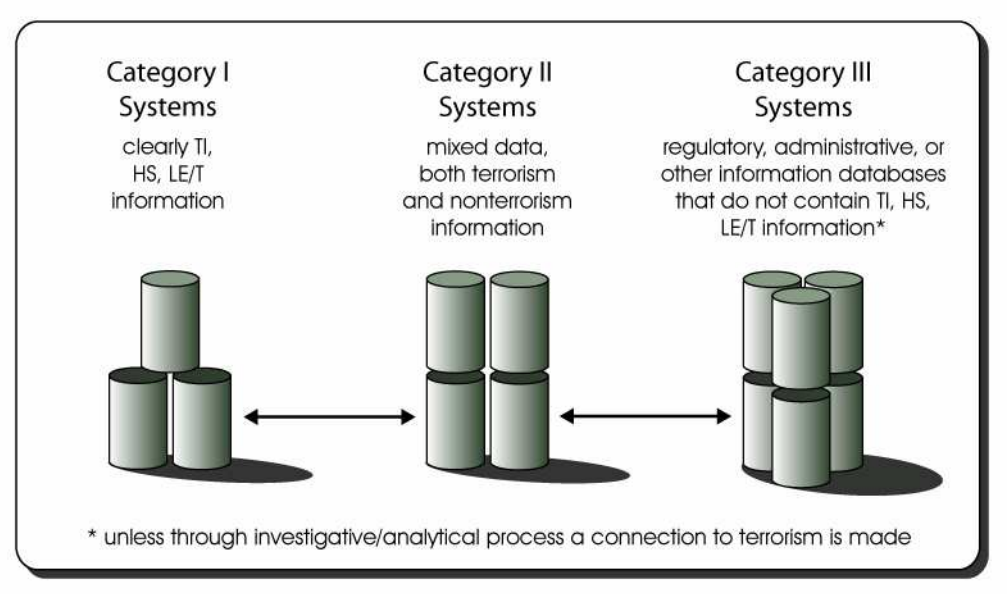
Approach:

Until such process is in place, it may be informative to identify different categories of systems and assess their applicability under the guidelines. There are three different categories that should be examined, which are identified as follows:

- Category I—Systems that are intended to exclusively contain terrorism information. Agencies were asked to identify terrorism systems as part of the development of the ISE Directory Pages, or Green Pages, which contain a list of systems that would fall mostly within this Category I. The Green Pages, however, should not be considered an exhaustive or entirely accurate listing of all Category I systems. They should, nonetheless, serve as a starting point in the process for agencies to identify Category I systems.
- Category II—Systems, including those used by the Intelligence Community and law enforcement, that are not designed to exclusively contain terrorism information but contain some terrorism information. In addition, other information may "become" terrorism information through the investigative/analytical process. Information that is or "becomes" terrorism information is subject to the ISE Privacy Guidelines if 1) it is protected information, and 2) it is shared. Examples of Category II systems include criminal history records and systems such as the Regional Information Sharing Systems and the Integrated Automated Fingerprint Identification System.
- Category III—Systems containing regulatory, administrative, or other information and that, on their face, do not contain any terrorism information. However, it remains possible that through the investigative/analytical process, connections may be made that relate information residing in such systems to terrorism. Information that "becomes" terrorism information in this manner is subject to the ISE Privacy Guidelines on the same basis as Category II information. Examples of Category III systems are benefits information and licensing files.

The first and third categories are relatively clear, and initial implementation should proceed on the basis that Category I systems must be conformed to the ISE Privacy Guidelines and that Category III systems will not likely need to be brought into conformity.

Until such time as a more definitive ISE process is established for identifying systems and sharing arrangements that form part of the ISE, the ISE privacy officials should proceed on the premise that, at least initially, agencies will need to make a preliminary identification of Category II systems.



The ISE Privacy Guidelines require that each agency identify its data holdings that contain protected information to be shared. In making determinations about Category II systems, it is important that a careful process be developed to address what, if any, system information will be shared and if shared, with whom it will be shared. These decisions will require a balancing of the privacy concerns and counterterrorism needs.

For purposes of applying the ISE Privacy Guidelines to Category II systems, a decision must first be made on whether or not data meets the ISE parameters. The PGC should provide guidance to agencies on how to begin an assessment of Category II systems that are known to contain some terrorism-related information in order to determine whether those systems contain 1) protected information and 2) especially sensitive personal information, such as medical, religious, or ethnic information. The PGC should also develop a checklist of criteria to assess the privacy and civil liberties issues involved with sharing those systems and how those issues can be addressed (e.g., via safeguarding mechanisms, training, access restrictions, and other privacy protection measures). This information will be important input when determining which databases should be shared within the ISE and how.

In short:

- Agencies should proceed with applying the ISE Privacy Guidelines to Category I systems, starting with the Green Pages listing.
- For Category II systems, ISE privacy officials should determine whether they contain protected information or especially sensitive information and should assess the privacy and civil liberties associated with sharing that will be used as input for the sharing determination.